Remarks

Applicants respectfully traverse and request reconsideration.

Claims 1-26 stand rejected under 35 U.S.C. §112, 2nd paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention. In particular, the Office Action indicates that it is not sure whether the selectable expiry data includes private key expiry. Applicants have suitably amended the claim to overcome this rejection.

Claims 1-4, 6-18, 23, 24 and 26 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Dolphin in view of Lewis (U.S. patent No. 5,761,306). Dolphin has been cited for teaching nearly all of the limitation of the claims. The Office Action indicates that Dolphin does not teach a system for public key updates. The Lewis reference has been cited as teaching a public key update system. In addition, official notice has been taken that public key certificates indicate validity periods for keys and are old and well known. Accordingly, the Office Action argues that it would have been obvious to combine the selectable validity period data of a non-public key update system of Dolphin with the public key update system of Lewis.

The Dolphin reference is directed to a system for access control for portable data storage media to facilitate, for example, secure periodic distribution of several different sets of information through the use of an access code. These decryption access codes are provided to users to allow users to gain access to distributed media. The Dolphin reference teaches one symmetric key for all users wherein different date ranges are associated with the same key depending upon the user. One encryption key is generated from a previous key. The Dolphin reference teaches that the access code or key may have expired for one user but the same key is still good for other users. Moreover, the key expiration date apparently used in the Dolphin reference relates apparently only to a public key and is not related at all to decryption keys or private keys. Since only one key is used for all users, Dolphin does not provide the security required for a public key infrastructure system as claimed by Applicants.

As to claims 1-4, 6-18, 20-24 and 26, Applicants claim, inter alia, selectable digital signature expiry data including both public verification key expiry data and selectable private signing key expiry data that are both selectable. The Dolphin reference appears to be silent as to providing updated digital signature key pairs and teaches using the same key for multiple users in contrast with Applicants' claimed invention. In addition, Applicants claim that the new encryption key pair (as in Claim 9) is not computable from a previous encryption key pair which again is completely different and distinct from the system taught in the Dolphin reference.

The Lewis reference is directed to a key replacement system in a public key cryptosystem. The Lewis system does not teach or suggest selectably varying key expiry data for digital signatures or encryption keys as claimed. In fact, Lewis is directed to a completely different problem. The Lewis reference is directed to securing replacement keys so that it is computationally difficult to determine a replacement key from its masked version. An active public key and a hash of a replacement public key is provided by a key server to nodes of the network. Each time a key request is performed, the active public key is discarded. A key replacement message is signed by an active private key and a replacement private key. Accordingly, the message is signed by a replacement private key from an entity that knows the replacement private key before the message is sent.

The combining of the Lewis reference with the Dolphin reference is improper. The Office Action appears to be using hindsight to combine distinctly different teachings in an attempt to obviate the Applicants' invention. For example, there is no teaching or suggestion in the Dolphin reference to use any other type of key other than the same key for multiple users, which is likely to potentially compromise the system. The Dolphin reference is not directed at all to digital signature expiry period control. In arguendo, even if the references were properly combinable, the resulting system would not operat4e properly. On the one hand, one symmetric key for all users needs to be used wherein date ranges are associated with the same key dependent upon each user, but the system,

according to Lewis, must use private keys that are apparently different for each user as required in a public key system. Applicants are unsure as to how such a combination of the system would properly function. Accordingly, Applicants respectfully request a showing of the teaching in either the Lewis or the Dolphin reference to combine such references or the motivation to combine such distinctly different systems to render obvious Applicants' claimed invention.

Claims 5, 19 and 25 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Dolphin and Lewis as applied to claims 1, 14 and 25 and further in view of the Applicants' prior art. Applicants reassert the arguments made above and further respectfully note that conventional public key cryptographic systems typically have a fixed default period that is the same for all clients on the system. The fixed default period is generally a fixed percentage of a total key lifetime that is not adjustable by a manager or certification authority. Applicants claim, inter alia, initiating, by a client unit, digital signature key pair update requests based on whether difference between a current data and a digital signature private key lifetime end date is less than an absolute predetermined period of time, and based on whether the difference between a current date and the digital signature private key lifetime end data is less than a predetermined percentage of the total duration of a digital signature private key lifetime. No such digital signature key pair update request or basis for such a request is taught or suggested in any of the references or the prior art. It is Applicants' own disclosure which teaches such an invention which provides many advantages over conventional systems. Applicants respectfully request a teaching in the references of such a digital signature key pair update request and the basis for initiating such a request as claimed.

For the reasons stated above, the applicants believes that claims are in condition for allowance and respectfully request that they be allowed. The Examiner is invited to contact the undersigned attorney by telephone or facsimile if the Examiner believes that such a communication would advance the prosecution of the present patent application.

Respectfully Submitted,

By: _____

Christopher J. Reckamp
Registration No. 34,414
Attorney for Applicants

Markison & Reckamp, P.C.
PO. Box 06229
Wacker Drive
Chicago, Illinois 60606-0229
Telephone: (312) 939-9800
Facsimile: (312) 939-9828